COMBINED FEDERATED BATTLE LABORATORY NETWORK
CFBLNet

Basic Guide to CFBLNet Initiatives Process

Version 1.0
December 2007

TABLE OF CONTENTS

CFBLNET OVERVIEW 2

Checklist 2
Description 3
Backbone Infrastructure (BLACKBONE) 3
BLUE Enclave 4
CFBLNet Unclassified Enclave (CUE) 4
Temporary Enclaves 4
Initiative Lead 5
Security 5
What is available to me? 5
Resources 5

HOW DO I GET INVOLVED (CIIP APPLICATION)? 6

CIIP Instructions 6
Step 1 6
Step 2 6
Step 3 6
Step 4 6
Step 5 7

INITIATIVE STAFFING PROCESS 8

Create Phase 8
Approval and Accredit Phase 9
Execute Phase 10
Final Report Phase 10

FREQUENTLY ASKED QUESTIONS - FAQ 11

CFBLNET OVERVIEW

The Combined Federated Battle Laborartory Network (CFBLNet) utilizes a global distributed Wide Area Network (WAN) as the vehicle to conduct unclassified and classified Initiatives. An Initiative is defined as being any collaborative experiment, trial, demonstration, training, de-risking exercise or other activity utilizing the CFBLNet. The Charter is amongst United States, Australia, Canada, New Zealand, United Kingdom and the North Atlantic Treaty Organisation (NATO) countries and organizations formed to promote and demonstrate C4ISR.

The CFBLNet consists of a distributed and integrated network architecture of Combined, Joint, and Service infrastructure components (networks, database servers, application servers, client workstations, etc.). These are located within the confines of the various CFBLNet Points of Presence (POPs), Battle Laboratories and Experimentation Sites of the Charter Members, which provide the applications, analytic tools, and communications necessary to conduct Initiatives. The USA Defense Information Systems Agency (DISA), centrally coordinates network and scheduling management in harmony with the CFBLNet Lead from the Initiative Leads (user or customer) plans.

Checklist

The checklist shows to the customer/user, the activities that are necessary to gain approval for the conduct of an Initiative over the CFBLNet. Further guidance is articulated within this document, detailed processes are contained within CFBLNet Publication 1 Annexes.

☐	Establish the lead nation/organization and produce an agreed Test Plan with all the Initiative participants.
☐	Prepare with your CFBLNet Lead a draft CFBLNet Initiative Information Package (CIIP), reflecting the agreed position and request your CFBLNet Lead Representative to submit it for approval.
☐	During the approval process, the security architecture will be reviewed by the CFBLNet Security Working Group for endorsement, subject to any revisions required.
☐	During the approval process, the CFBLNet Network Working Group will review your Initiative to determine the CFBLNet resources required. Such elements as connectivity, bandwidth, services, cryptos and key material, special requirements and engineering support will be considered and subject to meeting the correct criteria endorsement will be given.
☐	Security accreditation will be necessary from your national/organizational security accreditation authority for all participating Sites and the Initiative. This will then be elevated to the Multi-national Security Accreditation Board (MSAB) for final approval.
☐	The CFBLNet Secretariat will schedule your Initiative, into the Master Calendar.
☐	On being given approval for your Initiative the CFBLNet Engineers will be provided to support the testing, execution and tear-down phases.
☐	On completion – it is customary for the CFBLNet community to receive feedback from the customer on its performance including lessons learnt (a small questionnaire requires filling-in)

Table 1: Checklist Points for CFBLNet Approval

Description

CFBLNet Infrastructure & Mode of Operation

Figure 1 shows at a high level the POP topology for the CFBLNet.

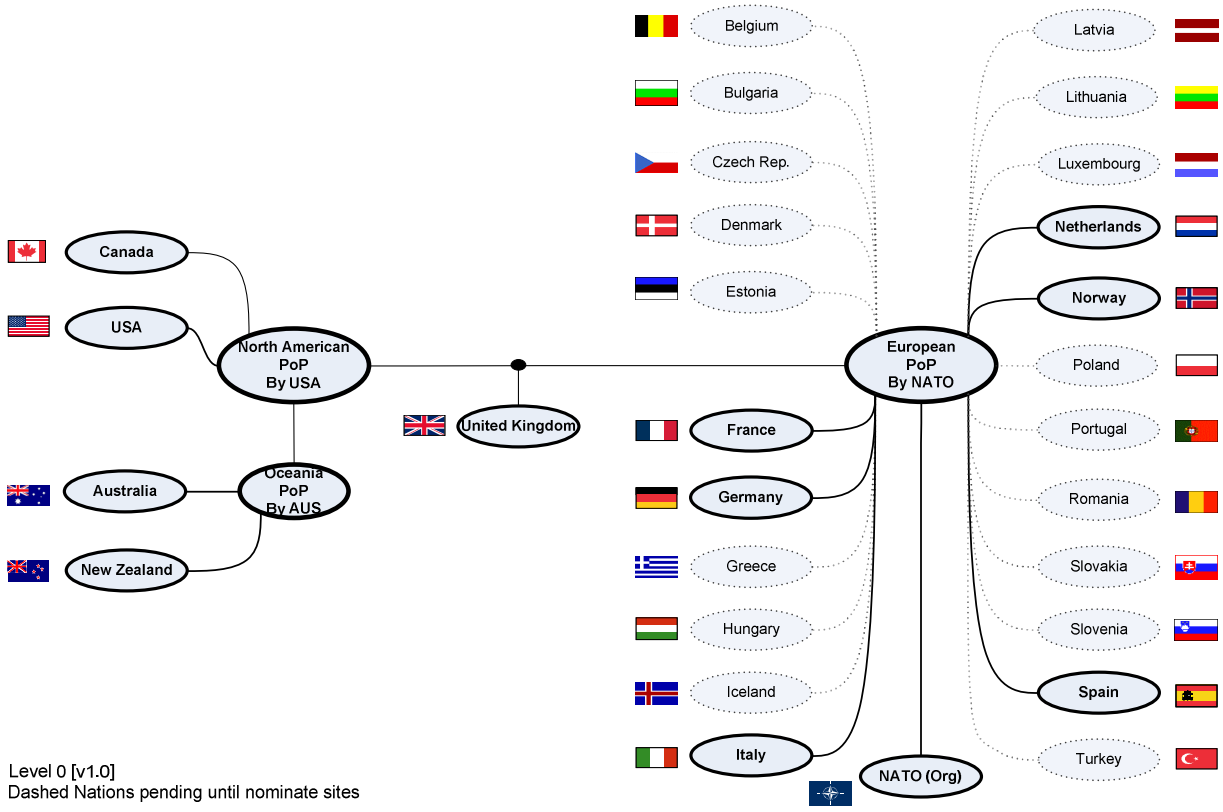

Figure 1: CFBLNet High Level Topology

The CFBLNet provides a networked environment between each chartered nation's/organisation's POP for the purpose of conducting Initiatives. Each nation/organization possesses its own infrastructure for connecting to government and defence sites/assets; these infrastructures can be used to conduct Initiatives. Your CFBLNet Lead will be able to inform of national distributive connections to any POPs.

The CFBLNet environment consists of the following components:

Backbone Infrastructure (BLACKBONE)

The BLACKBONE provides a common, closed, unclassified routed IP network layer implementation using a mixture of both ATM and IP bearer networks. Its primary purpose is to transport encrypted traffic throughout the network; this is used frequently to set-up bi-lateral or multi-lateral enclaves for Initiatives.

BLUE Enclave

A permanent classified IP routed logical network operating over the BLACKBONE. It will operate as a System High logical network at the SECRET level, releasable AUSCANNZUKUS + NATO.

CFBLNet Unclassified Enclave (CUE)

The CUE is a permanent enclave operating at the Unclassified - Non Releasable to Internet level, over the BLACKBONE.

Temporary Enclaves

An enclave created for a finite period to support the execution of specific Initiatives and operating over the BLACKBONE. The level of classification and release caveats used within these enclaves will be determined by the Initiative requirements.

Enclave confirmation is shown at figure 2.

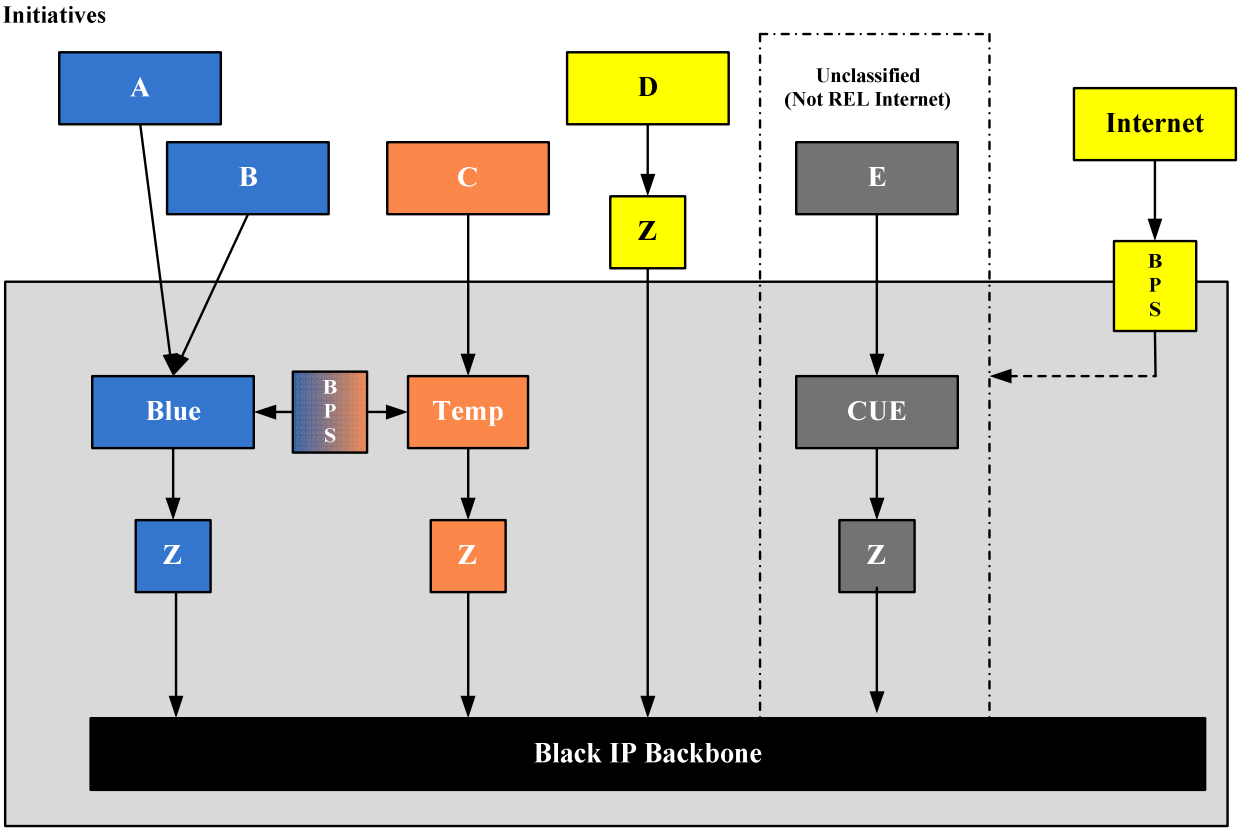

Figure 2: Description of CFBLNet Architecture

The coordination and provision of all network services within a specific temporary enclave will be the responsibility of the Initiative sponsor and is co-ordinated with the CFBLNet Network Working Group.

Initiative Lead

By definition an Initiative Lead is the selected head coordinator for and Initiative pulling together all Initiative Participant needs, for reporting to the CFBLNet Lead. The Initiative Lead and Initiative Participants are therefore users/customers of the CFBLNet.

Security

Each Initiative participant is responsible for implementing CFBLNet Security Policies and Procedures in conjunction with the National Accreditation Authorities (NAA) accreditation procedures. Participants will require security endorsement by the Multi-National Security Accreditation Board (MSAB), for site(s) and the Initiative(s) prior to connection to the CFBLNet.

What is available to me?

Inter-national connectivity and services under controlled security parameters and technical charters, this should make easy your requirements for inter-national information exchange.

Basic User Services for each enclave as required:

- Domain Name Service (DNS);
- E-mail (SMTP);
- Web (HTTP);
- Network Time Protocol (NTP) Source;
- News (NNTP);
- IP Telephony Call Manager;
- VOIP phone @ each site.

Resources

Initiative Participants are responsible for bearing their costs to participate in each Initiative in terms of manpower and project specific materials and services. In general the infrastructure and support from the CFBLNet POP for international connectivity is free of charge, this does vary from nations and organizations arrangements.

HOW DO I GET INVOLVED (CIIP APPLICATION)?

A draft CIIP is required to be prepared by the Initiative Lead in conjunction with the CFBLNet Lead.

CIIP Instructions

Step 1
You should first identify which nation/organization will lead for the Initiative. This nation/organization will then become the primary body responsible for the generation of the CIIP, which provides the essential details for the CFBLNet community to approve your Initiative.

Step 2
The CIIP is prepared and completed by the Initiative Lead with the assistance of their national CFBLNet Lead.

Step 3
It is mandatory for the Initiative Lead to complete Tabs 1 to 8 (colour coded banana yellow) with the details requested, please note Tabs 9 to 11 are CFBLNet use only:

Some of the key factors you will need to consider with your Initiative community to give a consolidated agreement prior to filling out the form are:

- The participating nations and sites of CFBLNet charter members and non-charter members – if any;
- POC details;
- Time schedule for CFBLNet usage;
- Network topology and cross domain connection;
- Information protective marking and/data release caveat;
- MOU and/or data sharing agreement;
- Network services and application.

Step 4
On completion give to your CFBLNet lead, who will then submit the CIIP for approval. A customer of the CFBLNet should expect from the submission of the CIIP the following times to gain approval from the CFBLNet authorities:

a. 45 working days for a non-complex Initiative where networking is straight forward, site accreditation is in place, together with the available provision of cryptos, key material, connectivity etc.

b. For more complex Initiatives where there are design iterations, multiple nations, perhaps cross boundary devices, lead times of up to 90 working days can be expected,

c. There may be occasions that long lead time items such as security accreditation, cryptos and sponsorship of non-chartered sites may cause extensions beyond 90 working days.

Step 5

During the lifecycle of the Initiative it is the responsibility of the Initiative Lead to inform the CFBLNet Lead of any changes. An assessment will be made to whether or not the CIIP will require re-submission.

INITIATIVE STAFFING PROCESS
(THE ROUTE THE CIIP TAKES FOR APPROVAL)

The CFBLNet Initiative staffing process is the means by which an activity is approved and hence supported for execution on the CFBLNet, it encompasses the entire life-cycle, to include security accreditation and final reporting.

A high level flow diagram of the CFBLNet Initiative staffing process can be seen at figure 3, together with details of the four phases.

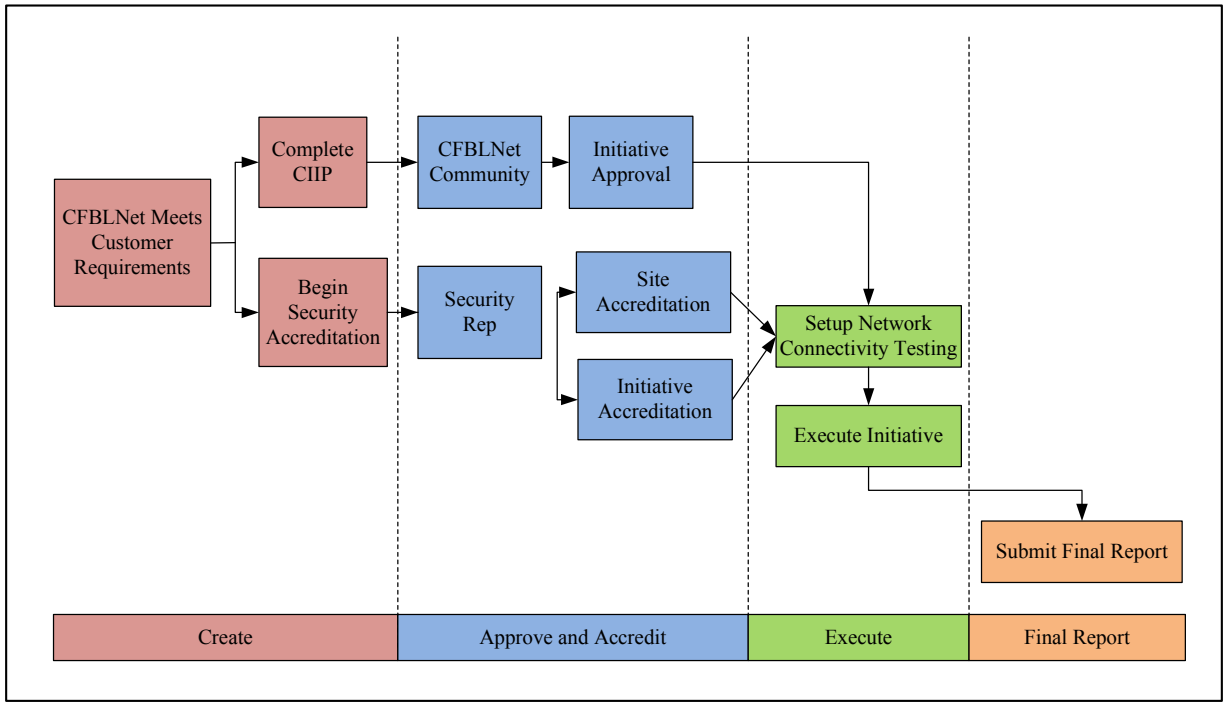

Figure 3: Flow Diagram of the CFBLNet Initiative Approval Process

Create Phase

Participants:	▪ Initiative Lead and Initiative Participants who will be conducting the Initiative (customer/user); ▪ CFBLNet Lead and his/her counterpart CFBLNet Leads who will be involved; ▪ National Accreditation Authority.
Input:	A draft CIIP.
Procedure:	This phase encompasses all preliminary staffing and scoping that will result in a consolidated CIIP; the Initiative Lead and CFBLNet Lead will work in conjunction to generate the CIIP and distribute to participants for initial agreement. It will include agreement on: ▪ All Initiative Participants are content to proceed with the architecture, resourcing, sites, security parameters and Initiative usage dates for the CFBLNet (build-up, execution and post execution tear down); ▪ All CFBLNet nations/organizations whose infrastructure is affected are in

	agreement; ▪ Confirmation of any security related issues (such as Information Sharing Agreements and MOUs); ▪ Any non-chartered participants must be identified; the procedure for addressing this is recorded at Annex C of CFBLNet Publication 1.
Output:	An agreed CIIP is submitted by the CFBLNet Lead to the CFBLNet Secretariat to commence approval

Approval and Accredit Phase

Participants:	▪ Initiative Lead and Initiative Participants who will be conducting the Initiative should any clarification or changes impact; ▪ CFBLNet Lead and his/her CFBLNet Lead who will be involved; ▪ National Accreditation Authority; ▪ Multi-National Security Accreditation Board (MSAB); ▪ CFBLNet Security Working Group; ▪ CFBLNet Network Working Group; ▪ CFBLNet Initiative Working Group; ▪ CFBLNet Secretariat; ▪ CFBLNet – Executive Group.
Input:	The CIIP
Procedure:	Initially the CIIP is distributed to all CFBLNet/Initiative Leads involved for formal agreement. The approval process can then be considered on two separate and simultaneous planes. ▪ One being the CFBLNet Networking Working Group review to establish the feasibility of the connectivity, services and Initiative timelines upon CFBLNet resources. Concurrently a CFBLNet Security Working Group review to consider and approve the Security architecture. ▪ The other being the Security accreditation axis to gain site(s) and Initiative(s) security accreditation and approval, this can be a long lead time therefore it is imperative to start early (involving NAA and MSAB). The CFBLNet Executive Group will finally endorse the Initiative with any relevant caveats.
Output:	▪ An approved CIIP scheduled for execution; ▪ Initiative - National Accreditation Approval Certificate (I-NAEC) from MSAB. This is the mandatory Initiative security approval required from all participants; ▪ Site – National Accreditation Approval Certificate (S-NAEC) from MSAB. This is the mandatory Site security approval required from all participants;

Execute Phase

Participants:	▪ Initiative Lead and Initiative Participants who will be conducting the Initiative; ▪ CFBLNet Lead and his/her CFBLNet Lead who will be involved; ▪ CFBLNet Networking Community; ▪ CFBLNet Secretariat for any re-scheduling.
Input:	▪ An approved CIIP scheduled for execution (test, execution and tear-down); ▪ I-NAEC – mandatory before connection; ▪ S-NAEC – mandatory before connection.
Procedure:	The Initiative participants with the CFBLNet Engineering community will prepare the environment for testing and execution as specified within the CIIP. Key Material distribution will also be implemented by DISA, NATO or National authorities as appropriate.
Output:	Execution results.

Final Report Phase

Participants:	▪ Initiative Lead and Initiative Participants should it be appropriate to let them review the feedback questionnaire; ▪ CFBLNet Lead; ▪ CFBLNet Secretariat.
Input:	Results of the Initiative execution.
Procedure:	Initiative Leads will be requested to fill-in a questionnaire (CIIP Tab 8) via the CFBLNet Lead to the Secretariat within 20 days of Initiative completion. This incorporates feedback to the CFBLNet community on any ways to improve its performance and also provides information with respect to operational benefits achieved by the Initiative.
Output:	Completed questionnaire (CIIP Tab 8).

FREQUENTLY ASKED QUESTIONS - FAQ

Question	*Answer*
Who is responsible for security and Intellectual Property Rights?	*The Initiative Sponsor is responsible for liaising with Initiative Participants to ensure that all data sharing agreements, MOUs to include Intellectual Property Rights, information exploitation, together with security aspects.*
Who helps me throughout the process to gain approval to use the CFBLNet?	*Your CFBLNet Lead will assist you to complete the CIIP and give advice on elements such as Security accreditation and CFBLNet connectivity and services provide.*
How does CFBLNet accredit a site?	*Your national/organizational accreditation authority accredits the site. You must work with them to prepare the paperwork. The National Accreditation Authority (NAA) sends a certificate to the MSAB. The MSAB issues a certificate to connect known as the S-NAEC.*
How does CFBLNet accredit an Initiative?	*The Initiative Lead deals with this with the CFBLNet lead, through the Local or National Accreditation Authority. The MSAB issues a certificate to connect known as the I-NAEC.*
Do I need accreditation for UNCLASSIFIED Initiatives?	*Yes.*
When should I start the security paperwork?	*As soon as you can. It can take from one to four months to get accredited.*
Where do I send the security paperwork?	*To your National Accreditation Authority (or NATO Office of Security for NATO). Your national/organizational lead can help you. In turn it will be forwarded to MSAB.*
How much does it cost?	*Discuss with your CFBLNet national/organizational lead.*
What nations/locations are connected to the CFBLNet?	*Your CFBLNet Lead can provide the high level CFBLNet Point of Presence topology and give guidance to the lower level national and organizational infrastructures.*
Is my partner site already online?	*Liaise with you CFBLNet Lead who will check.*
I want to connect to a particular nation, is this possible/how do I do that?	*Scope the situation with your CFBLNet Lead who will know the contacts to ask about particular nations and site. If CFBLNet is the answer to the question a CIIP will be required.*
What are the advantages of using CFBLNet as opposed to the Internet?	*Managed Service/Charter in Place/Experience level of support/different levels of classifications are available/established community and sites.*
How do I acquire technical details?	*Through your CFBLNet Lead*